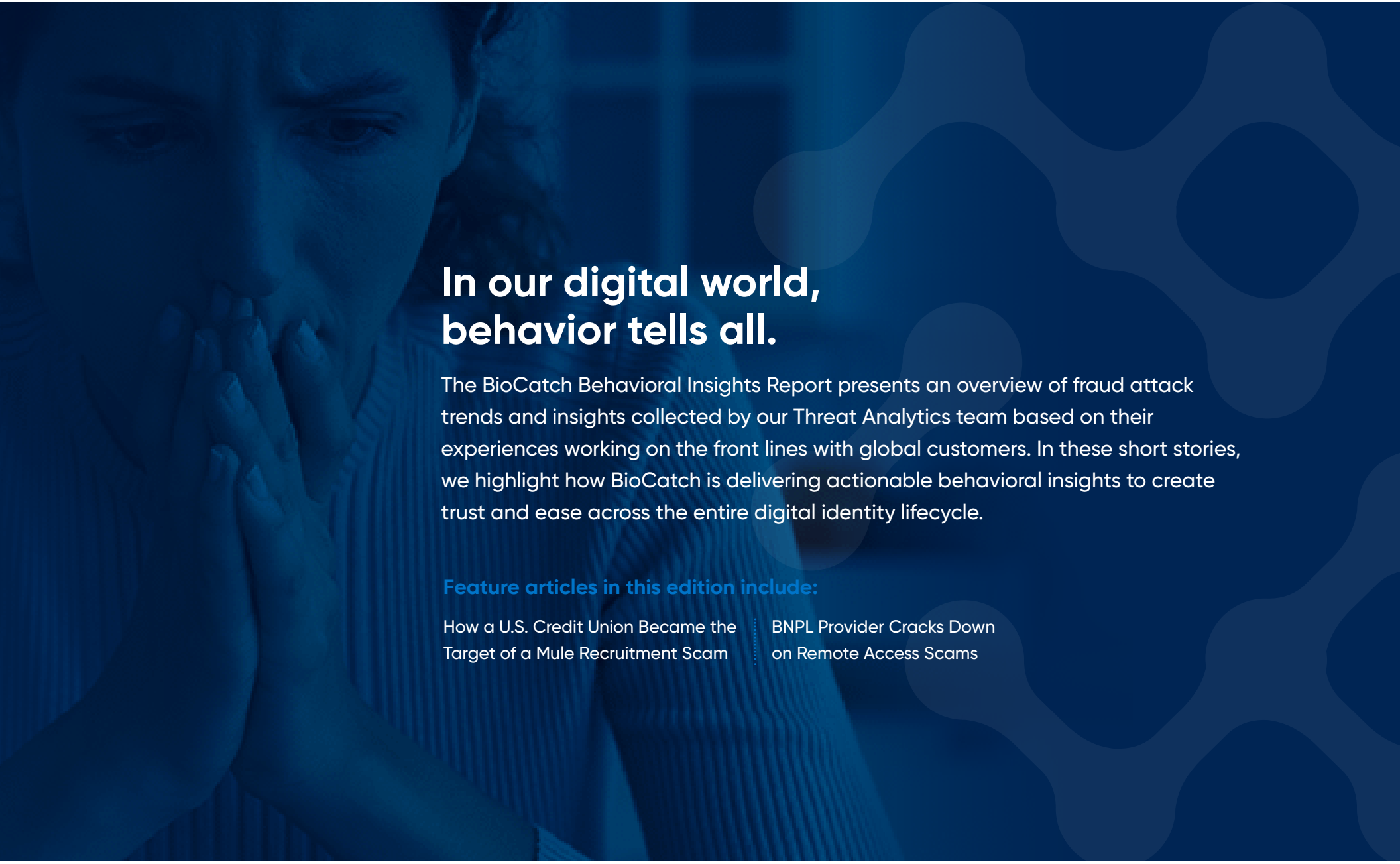
BioCatch

BioCatch Behavioral Insights:

Fraud Cases From the Wild

June 2023



In our digital world, behavior tells all.

The BioCatch Behavioral Insights Report presents an overview of fraud attack trends and insights collected by our Threat Analytics team based on their experiences working on the front lines with global customers. In these short stories, we highlight how BioCatch is delivering actionable behavioral insights to create trust and ease across the entire digital identity lifecycle.

Feature articles in this edition include:

How a U.S. Credit Union Became the Target of a Mule Recruitment Scam

BNPL Provider Cracks Down on Remote Access Scams

BioCatch

BEHAVIOR INSIGHT #1

How a U.S. Credit Union Became the Target of a Mule Recruitment Scam

A credit union that serves more than 300,000 members in the United States found itself the target of an active mule recruitment scam. The credit union became a hot topic on Telegram and Facebook with fraudsters advertising that they had access to customer bank accounts and would share profits with other fraudsters in exchange for a bank account to receive stolen funds.

However, the credit union informed us there was a job scam angle to this to recruit new mules. To scale the attack and recruit more mules, fraudsters were tricking unsuspecting job seekers by posting false advertisements on legitimate job boards promising work from home career opportunities. Often, the hiring process in these scams will be expedited without a detailed application or interview. With a weakening global economy where layoffs and inflation are on the rise, some people are desperate to earn cash, making them more susceptible to these scams.

In this scheme, the "job requirements" were to open an account with the credit union and download an app that gave the fraudster access to their phone information. Once the new account was established, the "employee" receives funds from existing valid customer accounts via internal transfers. Subsequently, the fraudster removes the funds using a variety of cashout methods including debit card transactions, P2P platforms (Zelle), Western Union wires, and money orders.

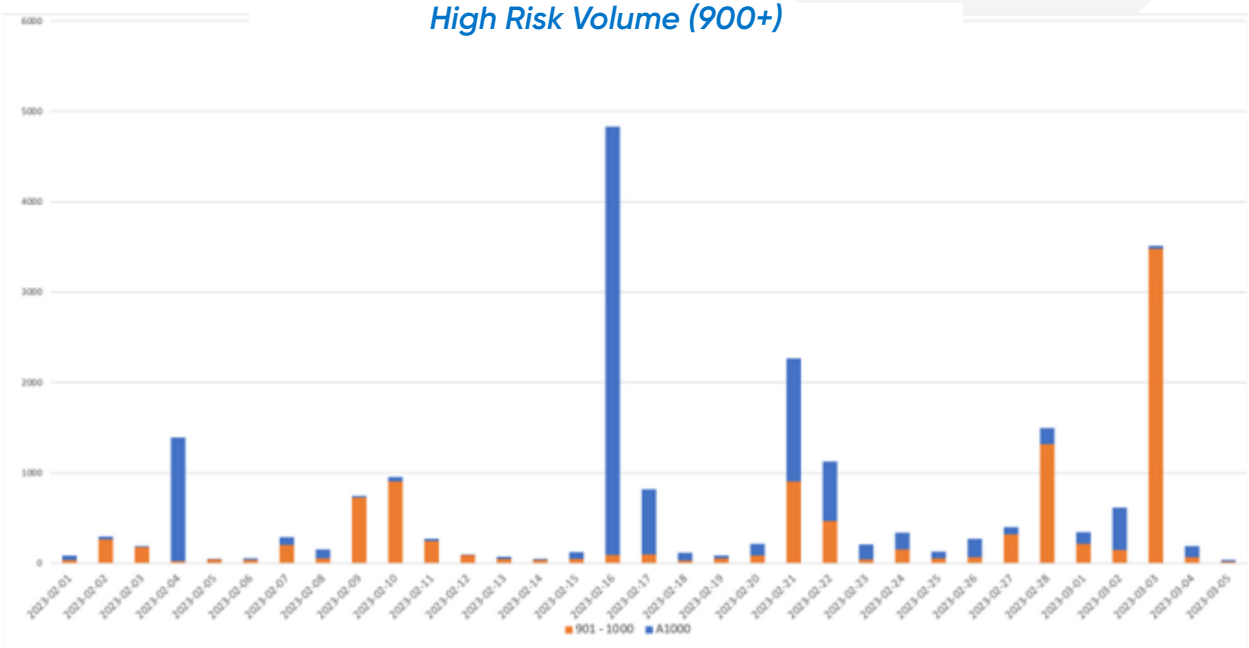
BEHAVIOR INSIGHT #1 How a U.S. Credit Union Became the Target of a Mule Recruitment Scam

Let's take a deep dive into an example of a fraud session from this event. Prior to the session below, the account was opened by the mule (legitimate applicant) and funds were transferred into the account (inbound payments). Subsequently, the process follows:

- Fraudster takes control of the account
- Immediately changes the authentication method
- Changes the email and phone number
- Adds a new payee
- Initiates two transfers totaling over $16,000 to fund other accounts at the credit union that are mules and operated by the fraudster
- Fraudster receives the funds and proceeds to cash out

On the surface, the attack seemed like other attacks we have seen before. Overall, the BioCatch ATO model identified these risky activities and scored them as high-risk with 91% of fraud capture at 900+ despite not being a typical case of account takeover. In the chart to the right, which plots the credit union's daily high scoring volume, there is a dramatic spike

High Risk Volume (900+)



of events scoring 1000, the highest BioCatch risk score, on February 16. The trend continues with an elevated level of high scores. The credit union ultimately incurred over $600,000 in losses over the course of two weeks in February.

At first, the credit union was not actively declining on 1000 risk scores. BioCatch made the recommendation to implement real-time decline rules for high-risk scores based on experience with other clients, and the fraud attack was mitigated.

BioCatch

BEHAVIOR INSIGHT #2

BNPL Provider Cracks Down on Remote Access Scams

Buy now, pay later (BNPL) services continue to boom, serving as an attractive alternative for consumers looking for convenient ways to pay for purchases over time. According to Juniper Research, spending on BNPL platforms will hit $437 billion by 2027, and the number of users is expected to surpass 900 million.

The lack of regulation or controls in the industry, along with the frictionless experience service providers have come to be known for, have caused BNPL platforms to serve as a lucrative target for fraudsters, and they are being exploited in very traditional ways. First, synthetic or stolen IDs are used to create fake accounts, exploiting offers and spending funds before anyone is wise to the con. Second, existing accounts can also be compromised leading to any available credit being spent on goods, services, and gift cards.

A large BNPL provider in Asia was already using the BioCatch Account Opening solution to prevent new account fraud. They approached us with a new problem: fraudsters were coercing customers to download remote access tools (RAT) through social engineering tactics and convincing customers to share their account credentials. Fraudsters were using a range of scripts to trick customers – from posing as a member of a bank's fraud team to PayPal security who were notifying the customer of suspicious behavior on the account. Each scheme had the same common end goal – to get the victim to install a remote access tool.

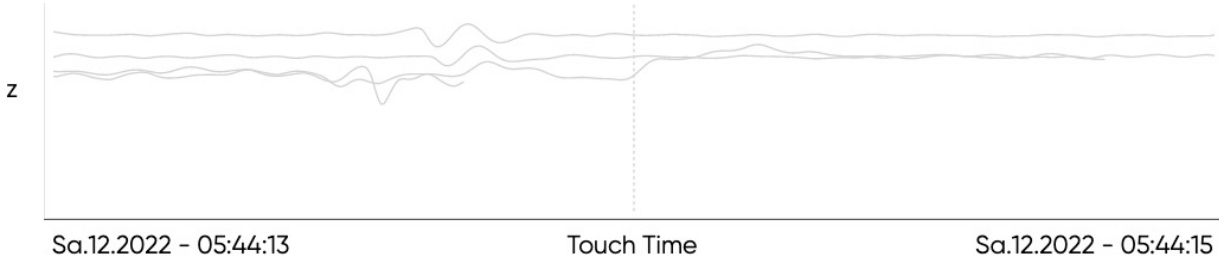
Behavioral biometrics can be used to detect the presence of a RAT during a live session. Indicators such as network delays, phone orientation, and behavioral patterns (no touches, constant pressure, excessive tap events, etc.) are measured to signal whether the device is operating via remote control. BioCatch has reported on similar events impacting other clients (see Additional Resources).

BEHAVIOR INSIGHT #2 BNPL Provider Cracks Down on Remote Access Scams

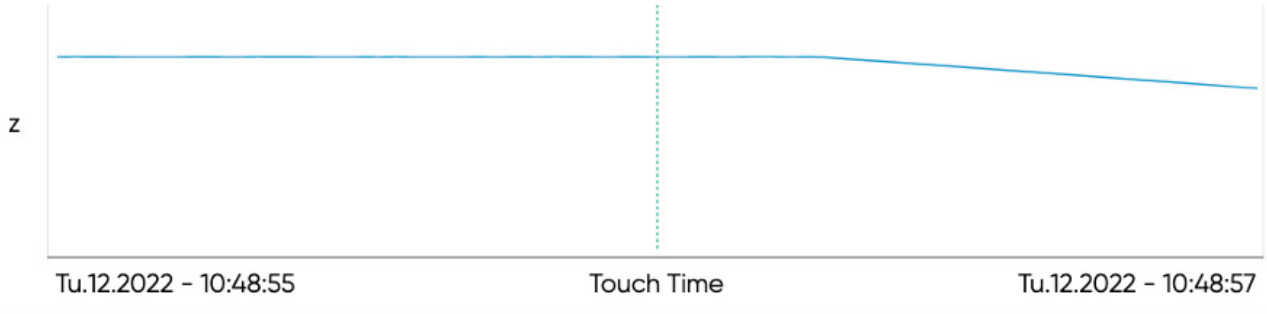
Putting a Remote Access Scam Under the Microscope

A good indicator to determine the presence of a RAT is phone orientation. Data collected from a mobile device's accelerometer and gyroscope can provides data points on device movement to determine whether a RAT is being used in a session. For example, the image below shows accelerometer movement of a genuine session represented by the gray lines. This shows natural movement of the device as a result of shaking, vibrations from pressing, device movement, and other expected human interactions. In the fraud session, the blue line shows no movement in any direction indicating the device is likely flat.

Genuine Session

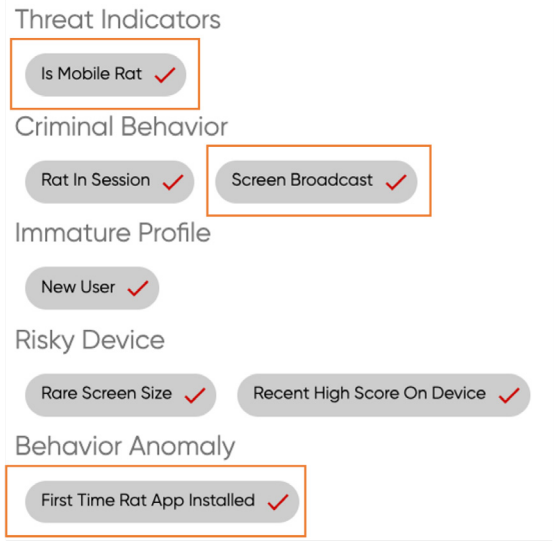


Fraud Session



BEHAVIOR INSIGHT #2 BNPL Provider Cracks Down on Remote Access Scams

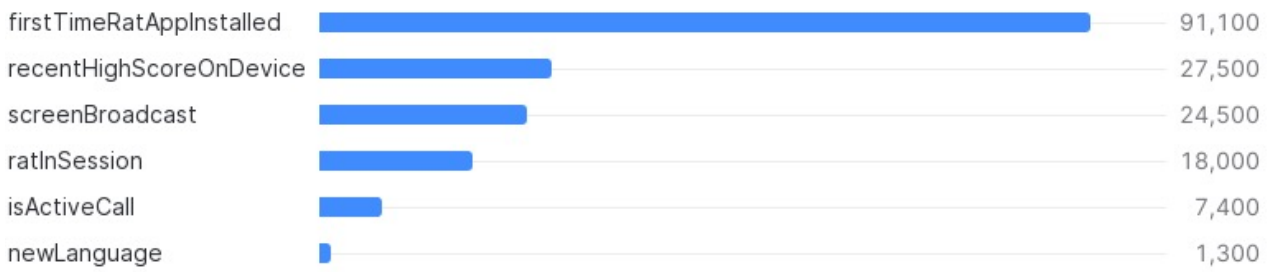
Another indicator to look at is installed applications (on Android devices). Most remote access scams will show a recently installed RAT app on the victim's phone. Combine this with other highly suspicious risk indicators, such as screen broadcasting while being on the phone at the same time, and we have the key ingredients for a remote access scam in progress. The image below outlines several risk indicators in a typical account takeover case involving remote access.



Even though BioCatch already works with several clients to detect remote access scams, the results were still shocking. Over 97% of fraud sessions returned a score of 900+, at an alert rate of 0.25%. In addition, 100% of fraud sessions marked as remote access scored 900+.

100% of fraud sessions marked as remote access scored 900+

Risk Factor Analysis – Index vs Fraud Population



An analysis of the top risk factors is insightful. In this case, BioCatch measures the proportionality of the risk factor within the fraud and genuine population – the higher the number, the more likely to see that risk factor in a fraud session. The chart above shows the risk factor 'First Time RAT App Installed' was highly prevalent in fraud sessions; in this specific instance, it was present in over 80% of fraud cases.

Fraudsters Abuse Legitimate Applications

It is not uncommon for fraudsters to abuse legitimate applications for nefarious purposes. This is the case with remote access scams where fraudsters convince victims to download a remote desktop application. In the case of the BNPL provider, two specific remote desktop applications were used in over 80% of all fraud cases. When compared to the genuine population, these applications are present on less than 0.1% of devices.

Additional Resources

Winning the RAT Race: How Banks Can Get Ahead of Remote Access Scams and Account Takeover Fraud

Top 5 Tips to Protect Customers From Remote Access Scams

BioCatch Behavioral Insights Report (January 2022 and March 2023) – reach out to your account manager or engagement manager for a copy.

About BioCatch

BioCatch is the leader in Behavioral Biometric intelligence and advanced fraud detection, leveraging technology built upon machine learning to analyze an online user's physical and cognitive digital behavior to protect individuals online. BioCatch's mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist. Today, BioCatch counts over 25 of the top 100 global banks as customers who use BioCatch solutions to fight fraud while transforming the consumer's digital experience. BioCatch's Client Innovation Board, an industry-led initiative including American Express, Barclays, Citi Ventures, and National Australia Bank, helps enable BioCatch to identify creative and cutting-edge ways to leverage the unique attributes of behavior for fraud prevention. With over a decade of analyzing data, more than 80 registered patents, and unparalleled research into human behavior, BioCatch continues to innovate to solve tomorrow's problems. For more information, please visit www.biocatch.com.

BioCatch